
ANTI-MONEY LAUNDERING POLICY

CIL SECURITIES LIMITED

REVISED ON 26.07.2025

ANTI MONEY LAUNDERING POLICY & PROCEDURES

1. Introduction

Parliament of India enacted Prevention of Money Laundering Act, 2002 (PMLA) to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto. The provisions of PMLA came into force on 01st July 2005. Section 12 of PMLA, inter-alia, requires all intermediaries associated with securities market and registered entities under section 12 of the Securities and Exchange Board of India Act, 1992 to maintain a record of all transactions and shall have to adhere client account Opening Procedures and maintain records of such transactions, which has been prescribed under the rules notified under the PMLA. Pursuant to this, Securities and Exchange Board of India (SEBI) issued Guidelines on Anti Money Laundering Standards and various circulars from time to time to implement the provisions of PMLA in the securities market and to prevent and impede money-laundering and combat financing of terrorism. CIL SECURITIES LIMITED (hereinafter referred to as 'CIL' or 'the Company'), hereby adopts and bring into effect this Anti Money Laundering Policy & Procedures (AML Policy & Procedures) in accordance with the provisions of PMLA and the rules made thereunder, SEBI Guidelines and Circulars issued from time to time on this subject. The policy applies not only to money laundering, but also to terrorist financing insider trading and substantial acquisition of securities or control as prescribed in Section 12 A read with Section 24 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) will now be treated as a scheduled offence under schedule B of the PMLA. All references to money-laundering in this policy, company policies and procedures and standards include terrorist financing as appropriate.

2. Back Ground:

2.1. The Prevention of Money Laundering Act, 2002 has come into effect from 1st July 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India..

2.2. As per the provisions of the Act, every banking company, financial institution (which includes chit fund company, a co-operative bank, a housing finance institution and a nonbanking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:

- All cash transactions of the value of more than Rs 10 lakhs or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency where such series of transactions take place within a month and the monthly aggregate exceeds an amount of 10 lakh rupees or its Equivalent in foreign currency.
- All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as demat account, security account maintained by the registered intermediary.
- All transactions involving receipts by non-profit organizations of value more than rupees ten lakh, or its equivalent in foreign currency;

- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- All suspicious transactions whether or not made in cash and by way of-
- Deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of—
- Cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
- Travellers cheques, or
- Transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
- Any othe(d) any other mode in whatsoever name it is referred to;
- Credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;
- Money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:-
 - (a) Payment orders, or
 - (b) Cashiers cheques, or
 - (c) Demand drafts, or
 - (d) Telegraphic or wire transfers or electronic remittances or transfers, or
 - (e) Internet transfers, or
 - (f) Automated Clearing House remittances, or
 - (g) Lock box driven transfers or remittances, or
 - (h) Remittances for credit or loading to electronic cards, or
 - (i) Any other mode of money transfer by whatsoever name it is called;
- (iv) Loans and advances including credit or loan substitutes, investments and contingent liability by way of:
 - (a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or
 - (b) purchase and negotiation of bills, cheques and other instruments, or

- (c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or
- (d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;
- (v) Collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.
- (a) All cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
- (b) All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

In Case Company finds any suspicious transactions including transactions integrally connected', 'transactions remotely connected or related' will be reported as per prescribed procedures. In case we find variance in CDD/AML standards prescribed by SEBI and the regulators, the company will adopt more stringent of the two.

3. Policies and Procedures to Combat Money Laundering and Terrorist Financing Policy

The Company shall endeavor at all times to comply, in letter and spirit, with the provisions of all relevant laws, rules, regulations, guidelines and circulars issued by regulatory authorities in relation to anti-money laundering and the Company's policies & procedures for prevention of Money Laundering and Terrorist Financing and ensure their effectiveness and compliance with all relevant legal and regulatory requirements.. To these ends the Company shall:

Appoint a Principal Officer responsible for ensuring compliance with the PMLA;

The Company has appointed a Designated Director as defined in Rule 2 (ba) of the PML Rules, who will be responsible for ensuring the compliance with the PMLA requirements;

"Designated Director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes the Managing Director or a Whole-time Director duly authorized by the Board of Directors

Establish appropriate 'Customer Due Diligence Process' for:

- identification of clients (and actual beneficial owners) and verification of their identity;
- obtaining additional 'know your client' information as appropriate and necessary;
- acceptance of clients;
- identification of suspicious transactions and reporting of the validated suspicions to the appropriate authorities, as required;

Maintain appropriate records of customer identification and trail of transactions; and Co-operate with the regulatory authorities to the extent required by the applicable laws and provide information as may be required, without breaching the customer confidentiality agreement;

Give appropriate training to the relevant staff for effective implementation of the AML Policy & Procedures.

Objectives

The objectives of this Policy are to:

Prevent and deter the use of the Company/Company's services by money launderers or those involved in criminal activities including financing of terrorism and to protect the reputation of the Company.

Protect the Company and its employees against unfounded allegations of facilitating money laundering and terrorist financing; and

Protect the Company and its employees against any criminal, civil and regulatory actions which might result from inadvertent involvement in money laundering and/or terrorist financing or from failure in operational controls.

3.1 Essential Principles

3.1.1. These Guidelines have taken into account the requirements of the Prevention of the Money Laundering Act, 2002 as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed guidelines in Part II have outlined relevant measures and procedures in preventing money laundering and terrorist financing. Some of these suggested measures and procedures may not be applicable in every circumstance. We should consider carefully the specific nature of its business, organizational structure, type of customer and transaction, etc. To satisfy itself that the measures taken by them are adequate and appropriate to follow the spirit of the suggested measures in Part II and the requirements as laid down in the Prevention of Money Laundering Act, 2002.

3.2 Obligation to establish policies and procedures

3.2.1. International initiatives taken to combat drug trafficking, terrorism and other organized and serious crimes have concluded that financial institutions including securities market intermediaries must establish procedures of internal control aimed at preventing and impeding money laundering and terrorist financing. The said obligation on intermediaries has also been obligated under the Prevention of Money Laundering Act, 2002. In order to fulfil these requirements, there is also a need for registered intermediaries to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

3.2.2. In light of the above, management is committed to establish appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The Registered Intermediaries should:

- (a) Issue a statement of policies and procedures, on a group basis where applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements;
- (b) Ensure that the content of these Guidelines are understood by all staff members;
- (c) Regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. Further in order to ensure effectiveness of policies and procedures, the person doing such a review should be different from the one who has framed such policies and procedures;
- (d) Adopt customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing;

(e) undertake customer due diligence (“CDD”) measures to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction; and

(f) Company is having system in place for identifying, monitoring and reporting suspected money laundering and terrorist financing transactions to law enforcement authorities and

(g) Develop staff members’ awareness and vigilance to guard against money laundering and terrorist financing.

4. Written Anti Money Laundering Procedures

Section 3 of PMLA has defined the “offence of money laundering” as under: “Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it is untainted properly shall be guilty of offence of money laundering”. Such procedures should include inter alia, the following specific parameters which are related to the overall ‘Client due Diligence Process’:

- a. Policy for acceptance of clients
- b. Procedure for identifying the clients
- c. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

5. Client Due Diligence

Elements of Client Due Diligence Policy

The objective is to ensure that:

- a. Obtains sufficient information about to the client in order to identify who is the actual beneficial owner of the securities or on whose behalf transaction is conducted.
- b. Verify the customer’s identity using reliable, independent source, document, data or information.
- c. Conduct on-going due diligence and scrutiny of the account / client to ensure that the transaction conducted are consistent with the client’s background / financial status, its activities and risk profile. Every year the financial statements to be taken on record for all corporate clients. Though it is not possible to know all the details and exact details of the client’s background and financial status, it should be our Endeavour to make a genuine attempt towards achieving this. This will be done in two ways:

Policy for Acceptance of Clients

· For New Clients:

- a) Each client should be met in person, before accepting the KYC. The client should be met at the Head Office or any of the branch offices as per mutual convenience of the client and ourselves.
- b) Verify the PAN details on the Income Tax website.
- c) All documentary proofs given by the client should be verified with original.
- d) Documents like latest Income Tax returns, annual accounts, etc. should be obtained for ascertaining the financial status. If required, obtain additional information/document from the client to ascertain his background and financial status.
- e) Obtain complete information about the client and ensure that the KYC documents are properly filled up, signed and dated. Scrutinize the forms received at our office thoroughly for account opening.

- f)** Ensure that the details mentioned in the KYC matches with the documentary proofs provided and with the general verification done by us.
- g)** If the client does not provide the required information, then we should not open the account of such clients.
- h)** As far as possible, a prospective client can be accepted only if introduced by existing client or associates or known entity. However, in case of walk-in clients, extra steps should be taken to ascertain the financial and general background of the client.
- i)** We should not open any accounts in fictitious / benami / anonymous basis.
- j)** We should not open accounts where we are unable to apply appropriate KYC procedures.
- k)** Company ensures with the 6 KYC attributes that will be mandatory to collect from all the categories of clients as per regulatory requirements
 - a) Name
 - b) Address
 - c) PAN
 - d) Valid mobile number
 - e) Valid email-id
 - f) Income range

apart from that nominee details of new and existing clients will be updated accordingly or nominee opt-out form will be collected

- l)** As per provisions of Income Tax Act -1961 the Company make sure that mandatorily all the PAN of the clients are seeded with their aadhar.

· For Existing Clients :

- a)** Review of KYC details of all the existing active clients in context to the PMLA 2002 requirements.
- b)** To verify status of client in KRA Agencies website and compliance at the time of account opening as per SEBI {KYC (Know Your Client) registration agency} Regulations, 2011,
- c)** Classification of clients into high, medium or low risk categories based on KYC details, trading activity etc for closer monitoring of high risk categories.
- d)** Keep updating the financial status of the client by obtaining the latest Income Tax Return, Networth Certificate, Annual Accounts etc.
- e)** Update the details of the client like address, contact number, demat details, bank details etc. In case, at any point of time, we are not able to contact the client either at the address or on the phone number, contact the introducer and try to find out alternative contact details.
- f)** Check whether the client's identity matches with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any local enforcement / regulatory agency. For scrutiny / back ground check of the clients / HNI, websites such as www.watchoutinvestors.com should be referred. Also, Prosecution Database / List of Vanishing Companies available on www.sebi.gov.in and RBI Defaulters Database available on

www.cibil.com should be checked. UNSC, 4. OFAC (Office of foreign Access and Control give by US Treasury department)

g) If a client is found matching with OFAC,UNSC or with SEBI Debarred list we not open the account and immediately informed to Principal Officer/ Designated Director for further action.

h) Scrutinize minutely the records / documents pertaining to clients of special category (like Non-resident clients, High Net worth Clients, Trusts, Charities, NGOs, Companies having close family shareholding, Politically exposed persons, persons of foreign origin, Current/Former Head of State, Current/Former senior high profile politician, Companies offering foreign exchange offerings, etc.) or clients from high-risk countries (like Libya, Pakistan, Afghanistan, etc.) or clients belonging to countries where corruption / fraud is highly prevalent.

i) Review the above details on an going basis to ensure that the transactions being conducted are consistent with our knowledge of customers, its business and risk profile, taking into account, where necessary, the customer's source of funds.

I. For client which is a trust

and Trusts:

Where the Client is Other than Induvial and Trust then Person having beneficial ownership will be identified by taking Reasonable Measures.

aa) The Company will take appropriate measures to identity of the natural person, (who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.) However controlling ownership interest means ownership of/entitlement to:

i.) More than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;

ii.) More than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

iii.) More than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

bb) In Case of any matter of doubt in clause (aa) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

cc) In case if there is no natural person found in clause (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

ii. For client which is a trust:

The Company will identify the beneficial owner of the Trust and will take all the responsible measures in identification of such persons through identity settlor of the trust.

Threshold:

The Trustee/Protector having more than 10% or more interest or any other natural person exercising ultimate effective control over the trust through a chain or control of Ownership.

iii. Exemption in case of listed companies:

It will not be necessary for the company to identify and verify the identity of shareholder and beneficial owner if the member of the Trust is a company listed in the stock exchange or is a majority-owned subsidiary of such a company

iv. Applicability for foreign investors:

While dealing with foreign investors' the company will adhere to clarifications issued vide SEBI circulars CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/ MIRSD/ 07/ 2013 dated September 12, 2013, for the purpose of identification of beneficial ownership of the client.

d) The Company will verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c).

e) The Company will understand the ownership and control structure of its client.

f) Company will Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the companies knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and

g) Company will periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

1. Customer Due Diligence (CDD) At The UCIC Level

"If an existing KYC compliant customer of the Company desires to open another account or avail any other product or service from us, fresh CDD will not be exercised as far as identification of the customer is concerned."

This update allows customers to enjoy seamless access to new services within the same institution without redundant identity checks. , which will RES can maintain a consolidated record for each customer, improving data management and reducing operational overhead.

2. Increased Monitoring For High-Risk Accounts

"High risk accounts have to be subjected to more intensified monitoring."

This adjustment urges the Company to invest in more sophisticated risk management systems, particularly for high-risk clients. Leveraging automated risk detection can enable proactive monitoring, reducing financial and reputational risks associated with money laundering.

3. Clarity On Periodic KYC Updation

To bring greater transparency to KYC update protocols, the revised guidelines emphasize both updation and periodic updation, indicating that KYC data should be refreshed at regular intervals or whenever new information is obtained from the customer.

4. Seamless KYC Data Sharing With Central KYC Records Registry (CKYCR)

"In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Company will upload/update the KYC data, at the time of periodic updation or earlier when the updated KYC information is obtained/received from the customer."

This will introduce a more interconnected KYC data management approach. It empowers Company with real-time, synchronized KYC data across institutions, allowing to access up-to-date customer information effortlessly.

5. Simplified Customer Identification Through KYC Identifier

“The Company will seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online.”

This simplifies the KYC process by eliminating unnecessary document requests and reducing friction for customers. However, Company will establish robust digital frameworks to access and manage KYC records from CKYCR efficiently.

Risk Profiling Of the Client :

The Company will accept the client based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher than average risk of money laundering or terrorist financing.

By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high risk client we have to apply higher degree of due diligence.

In order to achieve this, all clients should be classified in the following category; Low, Medium, High.

It is extremely important to understand that the financial risk is different from the Money laundering risk and this will be covered in the training sessions and other interactions that happen with staff in reference to Anti Money Laundering of CFT.

Risk-Based Approach

The clients may be of a higher or lower risk category depending on circumstances such as the client's background, type of business relationship or transaction etc. We should apply each of the clients due diligence measures on a risk sensitive basis. We should adopt an enhanced client due diligence process for higher risk categories of client. Conversely, a simplified client due diligence process may be adopted for lower risk categories of client. In line with the risk-based approach, we should obtain type and amount of identification information and documents necessarily dependent on the risk category of a particular client.

Risk Assessment

i. We shall carry out risk assessment to identify assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations Security Council Resolutions (these can be accessed at http://www.un.org/sc/committees/1267/aq-sanctions_listshtml and <http://www.un.org/sc/committees/1988/list.shtml>).

ii. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

Clients of special category (CSC)

Once the Account opening team has validated client against the customer acceptance policy, special

category check, then it is an appropriate time to allot a risk profile to the client.

It will be the responsibility of the Account opening team to understand if the client falls into the categories mentioned below;

1. NRI
2. HNI (High Net worth Clients are clients with disclosed net worth of Rs 1 Crore or more)
3. Trust / Charitable Organizations / NGO (Non-Government Organizations)
4. Close Family Share holdings or beneficial ownership
5. Politically Exposed Person (PEP) are individuals who have been entrusted with prominent public functions in foreign country
6. Company Offering foreign exchange offerings
7. Client in high risk Country
8. Non Face to face client
9. Client with dubious public reputation (Clients whose name appears in the wilful defaulters list, negative list of RBI, UNSC 1267, UNSC 1988, SEBI Debarred List,

Domestic PEP, Arbitration Awards and ANMI ABCD.

The list of the categories are basically special categories, this list could be reviewed and could have more categories.

If a client falls into any of the above categories the client should be marked as a “CSC”, client of special category and the risk level immediately should be allocated as “High”.

For clients that do not form under the special category mentioned above we take into account other details like Occupation of the client, age of the client.

Specific occupations of the client will mean that client will be marked as medium risk.

Medium Risk: Business, Agriculture, Student, Professional and Others.

Low Risk: The clients who are not covered in the high & medium risk profile are treated as Low risk Profile client.

Medium Risk: Individual and Non-Individual clients falling under the definition of speculators, Day Traders and all clients trading in Futures and Options segment.

In exceptional circumstances the KYC team may allot the “medium” risk to the client if there is a sufficient reason that the client should be above low and not high.

Review of Risk constantly after the On Boarding: The ongoing risk review can trigger the client’s risk to be upgraded based on the following parameters or events.

1. Change of the client relationship from Indian to NRI. The risk would be upgraded to “High”
2. If it is later realized that the client is a High Net Worth client. The risk would be upgraded to “High”

3. If in future it is known that a client is PEP then apart from seeking permission from the management to continue the relationship, the client should be immediately upgraded to High risk
4. If it is later realized or the existing client is registered foreign exchange dealer the client will have to be upgraded to High risk.
5. If a client is residing in a country which has been recently declared by the FATF as a high risk jurisdiction or an existing client moves base into a high risk jurisdiction then naturally in both the cases client will be immediately upgraded to “High” risk.
6. If a client registers the authorization or gives a power of attorney to operate his account to somebody else, in that case the account is to be upgraded to “High” risk
7. If it is realized by the management that the existing client’s reputation is tainted because of a SEBI debarred or any such announcement then the client will be upgraded to “High”
8. Any employee of the organization could alert the principal officer and request based on any news item or an event in the public domain which can lead the risk to be made High

Client identification procedure (CIP):-

To follow the Client Identification procedure we need to follow following factors:

The ‘Know your Client’(KYC) policy should clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

The client should be identified by using reliable sources including documents / information which is provided by the clients at the time of account opening. We should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

Appropriate Risk management systems to be put in place to determine whether the client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic database of PEPS.

Reasonable measures to be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the Guidelines. Each original document should be seen prior to acceptance of a copy.

Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority of the company.

SEBI has prescribed the minimum requirements relating to KYC for certain class of the registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, should frame their own internal guidelines based on their experience in dealing with their clients and legal requirements as per the established practices. Further, we should also maintain continuous familiarity and follow-up where it notices inconsistencies in the information provided. The underlying principle should be to follow the principles enshrined in the PML Act, 2002 as well as the SEBI Act, 1992 so that the intermediary is aware of the clients on whose behalf it is dealing.

Implementation of CIP will be initiated with insertion of PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), In which the procedure to maintaining verifying and of clients of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

The Company will strictly implement the Policies and Adhere to all the requirements for obtaining the minimum information/documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time). Irrespective of the amount of investment made by clients

Reliance on third party for carrying out Client Due Diligence (CDD)

i. The company may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

ii. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, it is clarified that the registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

6. Record Keeping

To comply with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars. Maintaining such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior. Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries should retain the following information for the accounts of their customers in order to maintain a satisfactory audit trail:

(a) The beneficial owner of the account;

(b) The volume of the funds flowing through the account; and

(c) For selected transactions:

- The origin of the funds;
- The form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.
- The identity of the person undertaking the transaction;
- The destination of the funds;
- The form of instruction and authority.

In terms of rules made under the PMLA Act, Company shall maintain a record of:

a) all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;

c) all cash transaction where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;

d) all suspicious transactions whether or not made in cash;

e) identity and current address or addresses including permanent address or addresses of the Client, the nature of business of the Client and his financial status; Provided that where it is not possible to verify the identity of the Client at the time of opening an account or executing any transaction, the banking company, financial institution and intermediary, as the case may be, shall verify the identity of the Client within a reasonable time after the account has been opened or the transaction has been executed.

7. Information to be Maintained

We should maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

- a) The nature of the transactions;
- b) The amount of the transaction and the currency in which it is denominated;
- c) The date on which the transaction was conducted; and
- d) The parties to the transaction

8. Retention of Records

Company has appropriate internal mechanism in order to comply with the rules and requirements of Rule 3 and Rule 9 of the PML Rules and other requirements as and when felt necessary. In a way and manner that allows easy and quick retrieval of data as and when requested by the competent authorities is 5 (Five) Years, However internal mechanism of the Company will preserve the data for a period of 8 (Eight) Years as per SEBI (Depositories and Participants) Regulations.

Ensures that all customers and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars. The following document retention terms should be observed:

(a) All necessary records on transactions, both domestic and international, Should be maintained for a period of 05 (Five) years prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars. However internal mechanism of the Company will preserve the data for a period of 8 (Eight) Years.

(b) Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of 8 (Eight) years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

(c) Where required by the investigating authority, certain records, e.g. client identification, account files, and business correspondence, shall be retained for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

(d) Suspicious records along with the records of the identity of clients shall be maintained and preserved for a period of 8 (Eight) years from the date of cessation of the transaction between the Client and intermediaries.

(e) In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

Records of Information reported to Director, Financial Intelligence Unit (India) (FIU – IND)

We maintain and preserve the record of information related to transaction whether attempted or executed, which are reported to director, FIU-IND as required under Rules 7 & 8 of the PML Rules, for a period of 8 (Eight) Years from the date of the transaction between the client and the intermediary.

9. Monitoring of Transaction:

Regular monitoring of transactions is required for ensuring effectiveness of the Anti-Money Laundering procedures. Special attention is required to all complex, unusually large transactions / patterns which appear to have no economic purpose. Internal threshold limits to specify for each class of client accounts and pay special attention to the transaction which exceeds these limits. The background including all documents, office records and clarifications pertaining to such transactions and their purpose to be examined carefully and findings thereof to be recorded in writing. Such findings, records and related documents to be made available to auditors and also to SEBI/Stock Exchanges/FIU-IND/Other relevant authorities, during audit, inspection or as and when required. These records are to be maintained for period of five years from the date of transactions between the client and intermediary.

It should be ensured that record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department. Further, the Compliance Department should randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not.

Medium Risk: The clients can be classified into the medium risk category depending on a lot of things like Client wise Large Turnovers, particular Script exposure / trading client's income range, trading pattern. If any of the client would satisfy the above criteria, depending on the criteria satisfied the same would be classified into medium or high risk.

High Risk: The clients of medium risk could be classified into the high risk category depending on excessive and further unusual, patterns like Client wise Large Turnovers, particular Script exposure / trading, client's income range, trading pattern. If any of the client would satisfy the above criteria, depending on the criteria satisfied the same would be classified into high risk.

10. Suspicious Transactions Monitoring and Reporting

For the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' need to be considered Suspicious transactions" means a transaction relating to deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical whether or not made in cash which to a person acting in good faith –

- (a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offense specified in the schedule to the act regardless of the value involved ; or
- (b) Appears to be made in circumstances of unusual or unjustified complexity or
- (c) Appears to have no economic rationale or bonafide purpose. or
- (d) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

All the Branches/business associates shall report all Suspicious Transaction to Compliance Department immediately on observation.

On basis of the alerts generated as above / on basis of continuous monitoring, Compliance department has to furnish the information of the suspicious transactions to the Principal Officer immediately.

Whether a particular transaction is suspicious or not will depend upon the background details of the client, details of the transactions and other facts and circumstances. Followings are the circumstance, which may be in the nature of suspicious transactions: -

- a) Clients whose identity verification seems difficult or clients appears not to co-operate;
- b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
- c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
- d) Substantial increases in business volume without apparent cause;
- e) Unusually large cash deposits made by an individual or business;
- f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- g) Transfer of investment proceeds to apparently unrelated third parties;
- h) Off market transactions in the DP account of the clients.
- i) High trading activity in the relatively illiquid scrips.
- j) Major trading activity in the Z and T to T category scrips.
- k) Options trading wherein client has booked unusual profit or loss which does not commensurate with the changes in the prices of underlying security in the cash segment.
- l) High exposures taken by client as compared to income levels informed by clients.
- m) Unusual transactions by "Client of Special category (CSCs)" and businesses undertaken by offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

Any suspicion transaction need to be notified immediately to the Money Laundering Control Officer or designated Principal Officer. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion.

All the Transactions which are rejected or aborted by the clients upon not showing the details or required documents irrespective of transection value and the relation with such customer could not be initiated. All such client details will be referred to STR's for further Compliance.

In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Principal Officer, compliance, risk and surveillance team should have timely access to customer identification data, CDD information transaction records and other relevant information. The Principal Officer shall report to the Board of Directors and to the Director Operations jointly. Further the employees shall keep the fact of furnishing information in respect of transactions referred to above strictly confidential with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

Clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards published by FATF on its website (www.fatf-gafi.org), which are categorized as "clients of Special Category" to be subjected to appropriate counter measures. Measures which include enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and application of enhanced due diligence at the time of expanding business relationships with the identified country or persons in that country to be implemented. Also steps to be taken to independently access and consider other publicly available information.

It is ensured that irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA 2002 , STR is filed if there are reasonable grounds to believe that the transactions involve proceeds of crime.

In Addition to the above Supplemental Guidelines for detecting Suspicious transaction under Rule 7(3) of Prevention of Money Laundering (Maintenance of Records) Rules 2005

With a view to Revise and Update Red Flag Indicators the following guidelines has been laid down by the Company

The Following Trusholds should be adhered and if verified the following data shall be shared as Red Flag Indicator (RFI) to the prescribed Authority in apporopriate timelines as per Annexure – A

S.no	Alert Source	Alert Indicator	Indicative Rule/ Scenario
1.	Transaction Monitoring	TM-11 Funds Received from Non- Clients	Single or Muntiple Transfer of funds are more than 1 Crore in a calender month in broker account from muntiple sources/ accounts which are not reported as Client
2.	Transaction Monitoring	TM – 12 Margine Trading	Sudden Increase in funding amount of Margine Trading Facility (MTF) Exposure <ol style="list-style-type: none"> 1. By More than 50% of MTF Exposure of previous Month and 2. With the Value of More than Rs. 10 Crores.
3.	Transaction Monitoring	TM-13 Off-Market transfer to Un-related Accounts (refer Note -1)	<ol style="list-style-type: none"> 1. Only for Reason Code/s <ol style="list-style-type: none"> a. Off Market sale b. Gift c. Donation and 2. Valuation as per debit transection will be >25 Lakhs and 3. Exclude Accounts with same PAN, Mobile and Email id same Bank details (IFSC + ac no) (same mobile / email/ Bank details in muntiple bank account will be treated as related account) and family flag is enabled and; 4. Valuation is > 5 times of Income Range
4.	Transaction Monitoring	TM-13A – Suspicious Off Market Credit and Debit [Refer Note no: 1]	<ol style="list-style-type: none"> 1. Customer receive credit/ Demat of 50000 shares or Shares worth Rs. 25 Lakhs by single Transection or Series of Transection in and ISIN and, 2. 80% of More or Credit Shares get debited by way of off Market transfer to 3 or more than 3 un-related accounts and,

			3. Only listed Entity Shares will be Considered for this Alert (Monthly frequency) short span of time within 30days.
5.	Transaction Monitoring	TM – 13B off Market Delivery in Unlisted Scrip (Refer Note no-1)	<ol style="list-style-type: none"> 1. Single or series of Transaction where more than 500000 unlisted Equity Shares have been transferred with in a period of 1 month and; 2. Off – Market Transfer with Reason Code “ Off – Market Sale, Donation and Gift will be Considered and; 3. Exclude Own account Transfer (First holder PAN) i.e transfer made through account transfer cum closure module and with reason code transfer to own accounts (Monthly frequency)
6.	Transaction Monitoring	TM – 13C Gift, Donation Related off-Market Transfer	<ol style="list-style-type: none"> 1. Transaction value of such Transaction is beyond 5 times of Income Range/ Networth (as updated in Demat Account) on higher side as provided by the BO and; 2. Listed Equity shares will be Considered and, 3. Debit transaction specific reason code > 5 Lakhs in Value and 4. For reason code/s <ol style="list-style-type: none"> a. Family Account transfer b. Gift c. Donations
7.	Transaction Monitoring	TM-13D Off Market transfer at Variance with Market Value	<ol style="list-style-type: none"> 1. Off Market Transfer with Reason Code “ Off Market Sale and, 2. Difference of +/- 50% Difference in consideration Value mentioned by B.O and prevailing market Value of Equity Shares and, 3. Only Listed Equity Shares will be Considered 4.

11. List of Designated Individuals/ Entities

Maintain updated list of individuals / entities which are subject to various sanctions / measures pursuant to United Nations Security Council Resolutions (UNSCR), available from the URL <http://www.un.org/sc/committees/1267/consolist.shtml>. all existing accounts ensure that no account is held by or linked to any of the entities or individual included in the list. Full details of account bearing resemblance with any of the individuals entities in the list shall immediately be intimated to SEBI and FIU-IND.

12. Procedure for freezing of funds, financial assets or economic resources or related services

1. The Company ensure that all the procedures laid down in Section 51A UAPA Order dated August 27 2009, is effectively implemented. As per point listed below.
 2. Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.
 3. The stock exchanges, depositories and registered intermediaries shall ensure effective and expeditious implementation of the procedure laid down in the UAPA Order dated August 27, 2009 as listed below
- (a) On receipt of the updated list of individuals/ entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals/ entities') from the Ministry of External Affairs (MHA)'; SEBI will forward the same to stock exchanges, depositories and registered intermediaries for the following purposes:

The Company will adhere all the rules and order subject to UN Sanction Measures forwarded by SEBI for following Purposes.

- (i) Company will have updated lists of individuals or entities listed in the schedule to the Order or holding any funds, financial assets or economic resources or related services held in the form of securities with them and company will have regular checks in frequent intervals and the data will be maintained in electronic form.
- (ii) In case if any client is found to be guilty under the PMLA provisions then the following procedure to be followed by the Company, will be as under:

If the particulars of any of customer/s match the particulars of designated individuals/entities, the Company shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer in their books to the,
Joint Secretary (IS.I),
Ministry of Home Affairs,
At Fax No.011-23092569.
And also convey over telephone on 011-23092736. The Company would also convey the information through e-mail at jsis@nic.in.
- (iii) Apart From above communication the company will also forward details to UAPA nodal officer of SEBI and FIU-IND through post/fax and through e-mail (sebi_uapa@sebi.gov.in). Officer on Special Duty, Integrated Surveillance Department,

Postal Address Details:

Securities and Exchange Board of India,
SEBI Bhavan,
Plot No. C4-A, "G" Block,
Bandra Kurla Complex,
Bandra (E), Mumbai 400 051

- (iv) The Company will restrict the designated individuals/entities from doing any financial transaction on the aforementioned Clients. Under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736, The details send in the post will also be conveyed in e-mail at jsis@nic.in.
- (v) Company will also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph 12 (ii) as per format prescribed by regulators.
- (b) On receipt of the particulars as mentioned in paragraph 2.9.3 (a) (ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by the stock exchanges, depositories, registered intermediaries are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by stock exchanges, depositories, registered intermediaries are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.
- (c) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned depository under intimation to SEBI and FIU-IND. The order shall take place without prior notice to the designated individuals/entities.
- (d) Implementation of requests received from foreign countries under U.N. Securities Council Resolution 1373 of 2001.**
 - i. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.
 - ii. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.
 - iii. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officer in SEBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.
 - iv. Once the company will receive the requests from UAPA nodal officer of IS-I division as detailed in paragraphs 2.9.2 (a) and (b) of SEBI Circular SEBI/HO/MIRSD/ DOS3/CIR/P/2018/104.
 - v. The freezing order will take place by the company without prior notice to the designated person involved.

(e) Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

In Case if the applicant comes with evidence that the freezed accounts are inadvertently frozen than an application in writing from should be taken from the individual/entity with full details of Asset frozen given informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, and within time period of two days all such documents will be forwarded to -

- i) To the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 5(ii) above.
- ii) The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA.

If the given evidence suffice, and the regulators are satisfied. Than he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant. And accounts will be Un-frozen. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

d) Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

i. All Orders under section 51A of the UAPA relating to funds, financial assets or economic resources or related services, would be communicated to stock exchanges, depositories and intermediaries through SEBI.

The Company would inform the IS-I Division of MHA so that they may take effective action like informing the State Police and /or the Central Agencies for conducting the verification of the individuals/ entities identified by the registered intermediaries.

The Company to provide full support to the appointed agency for conducting of the verification so that the verification gets completed within a period of 5 working days.

The Company would not provide any prior notice to the designated individuals/entities

13. Reporting to Financial Intelligence Unit – India (FIU-IND):

Principal Officer (Director) of the Company shall act as a central reference point in facilitating onward reporting of transactions to FIU-IND and for playing an active role in the identification and assessment of potentially suspicious transactions. Principal Officer of the Company shall submit In terms of the PML Rules, intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Tower-2, Jeevan Bharati Building,
Connaught Place, New-Delhi – 110001
<http://fiuindia.gov.in/>

The Company will carefully go through all the reporting requirements and formats that are available on the website of FIU – IND under the Section Obligation of Reporting Entity – Furnishing Information – Reporting Format (https://fiuindia.gov.in/files/downloads/Filing_Information.html). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents While detailed instructions for filing all types of reports are given in the instruction

1. Cash Transaction Reports (CTRs): The Company will File Cash Transaction report for each month (If applicable) and submit it to FIU-IND by 15th of succeeding month
2. Suspicious Transaction report as prescribed under Rule 3 notified under the PMLA to; The Company will submit STR within 7 days of arriving at conclusion that any transaction whether cash or non-cash or series of transaction integrally connected are of suspicious nature it shall be ensured that there is no undue delay in arriving at such conclusion.
3. The Company will submit the Non-Profit Organization Transaction Reports (NTRs) for each month (If applicable) to FIU-IND by 15th of Succeeding month.
4. The Principle Officer of the company will stand responsible if any of Compliance has not been initiated in timely manner. In relation to submission of CTR, STR and NTR to FIU-IND;
5. The Company will maintain confidentiality in filing of CTR, STR and NTR to FIU-IND.
6. Company will not submit nil reporting to FIU-IND in case there are no cash/ suspicious/ non – profit organization transactions to be reported.

It is clearly stated that the company will not disclose any of the operations in the accounts where an STR has been made at any point of time. And all directors, officers and employees (permanent and temporary) are prohibited from disclosing, (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. And company clearly assures that there is no tipping off to the client at any level.

Company will also abide with a rule that irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if it has reasonable grounds to believe that the transaction involve in proceeds of crime.

14. Designation of an Officer for Reporting of Suspicious Transactions:

The Company has designated Mr. Ashok Kumar Inani (Director-Finance/ CFO) as the Designated Director to ensure overall compliance with the obligations imposed under chapter IV of the PMLA Act and the Rules. The Designated Director will ensure filing of necessary reports with the Financial Intelligence Unit (FIU –IND). The company has appointed Mr. K K Maheshwari (Managing Director) for Trading DP Stock Broker sub broker share transfer agent and merchant banker as the Principal Officer. as per rule 2(1) the Principle Officer is of higher management level, The Principal officer appointed would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including email addresses) of ‘Principal Officer’ including any changes therein shall also be intimated to the Office of the Director-FIU. As a matter of principle, it is advisable that the ‘Principal Officer’ is of a sufficiently senior position and is able to discharge the functions with independence and authority.

Appointment of Principal Officer:

The company has appointed Mr. K K Maheshwari (Managing Director) as the Principal Officer, as required under the Prevention of Money Laundering Act, 2002. The Principal Officer is responsible to discharge the legal obligations to report suspicious transactions to the authorities. The Principal Officer will act as a central reference point in facilitating onward reporting of suspicious transactions and assessment of potentially suspicious transactions. In case of any change in the Principal Officer, the information regarding the same would be immediately be informed to FIU.

15. Appointment of a Designated Director

As defined in Rule 2 (ba) of the PMLA Rules, the company shall appoint a Designated Director who should be responsible for ensuring the compliance with the PMLA requirements;

“Designated Director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes – the Managing Director or a Whole-time Director duly authorized by the Board of Directors if the reporting entity is a company.

As Per terms of 13(2) of PMLA, the director, FIU-IND can take appropriate action including levying, monetary penalty on designated director on failure of company to comply with any of its AML/CFT obligations.

Company had communicated the details of designated director to the director of FIU-IND

16. Employees’ Hiring/Training and Investor Education

Hiring of Employees

Adequate screening procedure has been in place to ensure high standard while hiring the employees with regards to competency level. The staff should be provided adequate training to understand the AML and CFT procedures. Training must be given by Professional either from within or outside the organization.

Training

All new staff, whether permanent, temporary or on contract, who may be involved in handling customers’ on-boarding, execution of transactions must receive suitable induction training to ensure that they fully understand their responsibilities under the Company’s AML Policy & Procedures. Such training shall inter-alia cover following topics:

- What is money-laundering?
- Company’s requirements and obligations under the AML Policy & Procedures.
- Company’s legal or regulatory requirements and the risk of sanctions/penalties for staff as well as the Company.
- Reporting requirements as prescribed by SEBI.
- The role played by Company’s Principal/Compliance Officer in money laundering deterrence.
- The need to protect the Company’s reputation.
- (i) Staff in high-risk areas should receive appropriate training to enable them to understand the anti-money laundering techniques which are likely to be used in the area, and to remind them of their personal responsibilities under the Policy and local legal requirements.

Annual refresher training courses should be conducted for staff in high-risk areas to remind them of their responsibilities and alert them to any amendments to the Company’s AML Policy & Procedures or local legal and/or regulatory requirements, as well as any new anti-money laundering techniques being used.

Investors Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. There is, therefore, a need for us to sensitize customers about these requirements as the ones emanating from AML and CFT framework. We would prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the AML/CFT programme.

Review Policy :

This policy shall be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs.

Above said policies reviewed by us on regular basis by our senior officials (other than the official who originally drafted the policy and keep it updated as per the various amendments in the PMLA rules.

Approval Authority:

This policy shall be approved by our Board of Directors.

Other Points

The Policy will be reviewed once in a year or as and when required and will be presented before the Board.

The Company has made the PMLA policy which is informed to the Investors through the Company's website and the company is also carrying out Investor Education initiative by explaining the investors about the PMLA rules & requirements.

Policy communication:

A copy of this policy shall be made available to all the relevant staff/persons such as: compliance Officer / department in-charge of registration of clients and sub-broker /authorized persons.

Further Information

Any queries or doubts concerning Company AML Policy & Procedures or any local legislation or regulation or Circulars or Guidelines relating to Anti Money Laundering and/or Combating Financing of Terrorism shall be referred to the Principal Officer of the Company.

Mr. Krishna Kumar Maheshwari

Sd/-

**CIL Securities Limited
214, Raghava Ratna Towers,
Chirag Ali Lane, Abids,
Hyderabad – 500001**

**This Policy is revised by Mr. Vinod Kumar Sabavath and
Reviewed by Mr. Krishna Kumar Maheshwari**

Date: 26th July, 2025

Place : Hyderabad